



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

Which output was taken on a VM running in Azure?

- A.

```
C:\Users\azadmin>arp -a

Interface: 10.0.1.5 --- 0x2
Internet Address      Physical Address      Type
10.0.1.1              01-23-45-67-89-AB    dynamic
10.0.1.255           ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-05-00-00-02    static
```
- B.

```
C:\Users\azadmin>arp -a

Interface: 192.168.0.5 --- 0x2
Internet Address      Physical Address      Type
192.168.0.1          12-34-56-78-9A-BC    dynamic
192.168.0.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-05-00-00-02    static
```
- C.

```
C:\Users\azadmin>arp -a

Interface: 172.16.0.5 --- 0x2
Internet Address      Physical Address      Type
172.16.0.1           AB-C0-12-34-56-78    dynamic
172.16.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-05-00-00-02    static
```
- D.

```
C:\Users\azadmin>arp -a

Interface: 10.0.1.5 --- 0x2
Internet Address      Physical Address      Type
10.0.1.1              d8-34-99-c5-0A-BC    dynamic
10.0.1.255           ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-05-00-00-02    static
```

Suggested Answer: D

Community vote distribution

A (40%)



B (40%)

D (20%)

  SingSingHK 1 month ago


Selected Answer: B

Study guide say so
upvoted 1 times

  Powers22 1 month, 3 weeks ago

Selected Answer: B

Every ARP request you send out on a Azure Virtual Network asking the MAC address for a specific IP address is always answered with the same simple MAC address: 12:34:56:78:9a:bc. This ensures all traffic reaches the Azure SDN Virtual Router
upvoted 1 times

  GAP77 2 months, 2 weeks ago

Selected Answer: A

I did the validation in a lab environment and got these results, which leads me to say that the correct answer for me is option A.

C:\Usersers admin>arp -a

Interface: 10.0.1.5 --- 0x6

Internet Address	Physical Address	Type
10.0.1.1	12-34-56-78-78-9a-bc	dynamic
10.0.1.255	ff-ff-ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-00-16	static
224.0.0.251	01-00-5e-00-00-00-fb	static
224.0.0.252	01-00-5e-00-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff-ff-ff	static

upvoted 2 times

  **zufyozirke** 3 months ago

Selected Answer: D

The giveaway is the MAC you see for the default-gateway (10.0.1.1). In Azure every VM talks to a virtual router so your ARP will always resolve .1 to the fabric’s MAC, not to your on-prem router’s OUI. Only output D shows a “weird” randomized MAC (D8-34-99-C5-0A-BC) for 10.0.1.1 – exactly what you’d see in Azure.

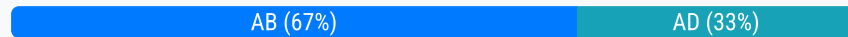
upvoted 1 times

When you deploy a single FortiGate VM using the available template from the Azure Marketplace, several other resources are also created. Which two resources, among others, are created during the process? (Choose two.)

- A. Two virtual NICs
- B. One NSG for each interface
- C. One VM Scale set
- D. One new route table

Suggested Answer: *AB*

Community vote distribution



🗨️ 👤 **GAP77** 2 months, 2 weeks ago

Selected Answer: AD

A and B are correct, for a single-VM we do not need a scale set and a NSG is created for all vNICs not one for each vNIC.
upvoted 1 times

🗨️ 👤 **zufyozirke** 3 months ago

Selected Answer: AB

When you launch the single-VM FortiGate from the Marketplace you get:

- A. Two virtual NICs. One for the public/internet side and one for the private/data side.
- B. One NSG for each interface. The template auto-generates an NSG tied to each NIC to lock down traffic.

You do not get a VM Scale Set (that's used by the autoscale template) nor a new route table by default in the single-VM deploy.
upvoted 2 times

Which role does the local network gateway play in FortiGate to Azure VPN connectivity?

- A. It manages the encryption keys for the VPN connection
- B. It represents the Azure VPN Gateway in the FortiGate configuration
- C. It defines the IP addresses of the on-premises network
- D. It is responsible for load balancing traffic between FortiGate and Azure

Suggested Answer: *C*

Community vote distribution



🗨️ 👤 **zufyozirke** 3 months ago

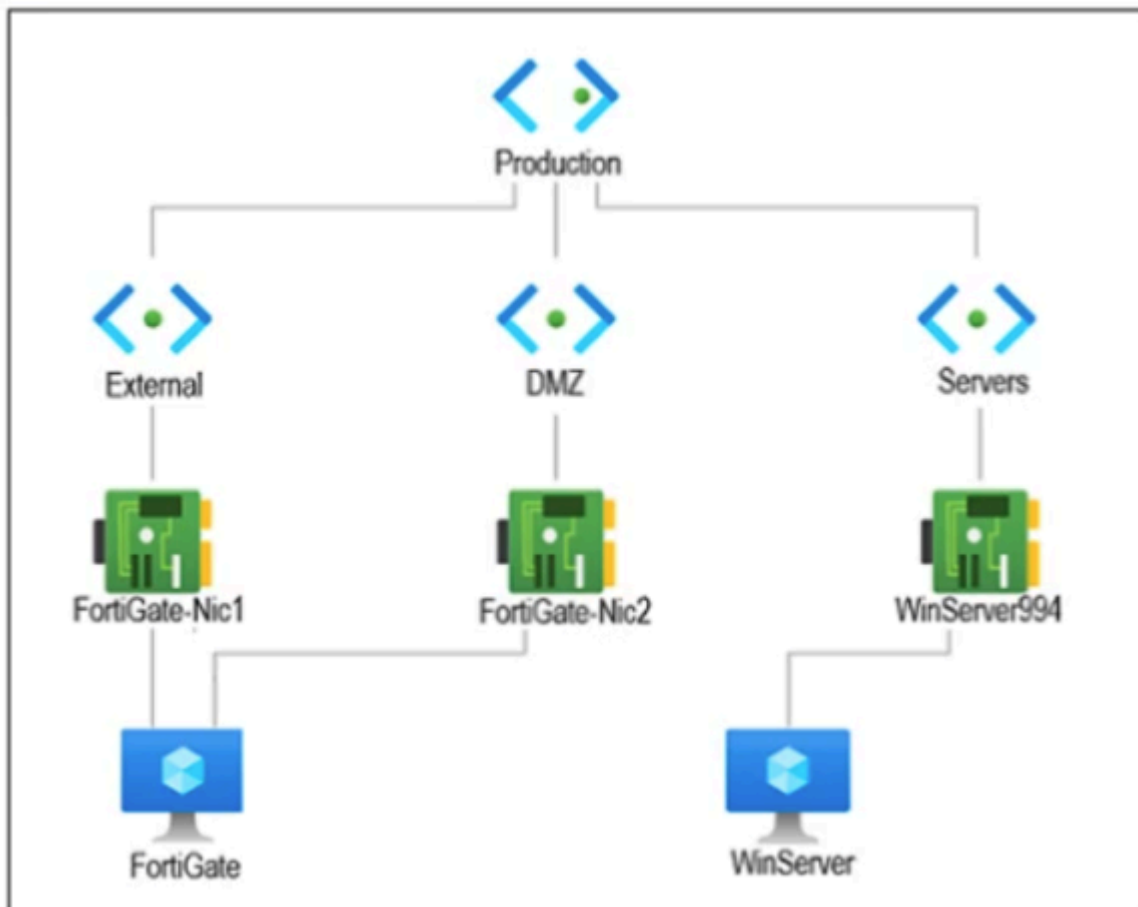
Selected Answer: C

The Local Network Gateway in Azure simply holds the details of your on-prem network (its public IP and the address prefixes you're advertising). In other words, it's used to define which IP ranges exist on the "local" side of the VPN.

Answer: C

upvoted 2 times

Refer to the exhibit.



You are troubleshooting a network connectivity issue between two VMs that are deployed in Azure.

One VM is a FortiGate that has one interface in the DMZ subnet, which is in the Production VNet. The other VM is a Windows Server in the Servers subnet, which is also in the Production VNet. You cannot ping the Windows Server from the FortiGate VM.

What is the reason for this?

- A. You have not created a VPN to allow traffic between those subnets
- B. By default, Azure does not allow ICMP traffic between subnets
- C. The firewall in the Windows VM is blocking the traffic
- D. You have not configured a user-defined route for this traffic

Suggested Answer: C

Community vote distribution

C (100%)

zufyozirke 3 months ago

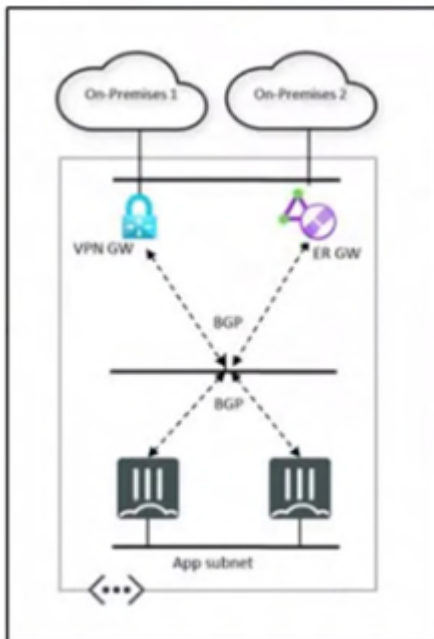
Selected Answer: C

Since both VMs live in the same VNet, Azure automatically handles inter-subnet routing (no VPN or UDR needed) and NSGs allow VNet traffic—including ICMP—by default. The only thing left is the OS firewall on the Windows box, which by default blocks ping.

Answer: C

upvoted 2 times

Refer to the exhibit.



In an expanding corporation, the different branches share resources connecting to Azure through Azure VPN Gateway and ExpressRoute Gateway. Which Azure solution can you implement to simplify and centralize the seamless sharing of the dynamic routing between FortiGate VMs and branches?

- A. Azure Route Server
- B. Azure Traffic Manager
- C. Azure Virtual Hub
- D. Azure Virtual WAN

Suggested Answer: A

Community vote distribution

A (100%)

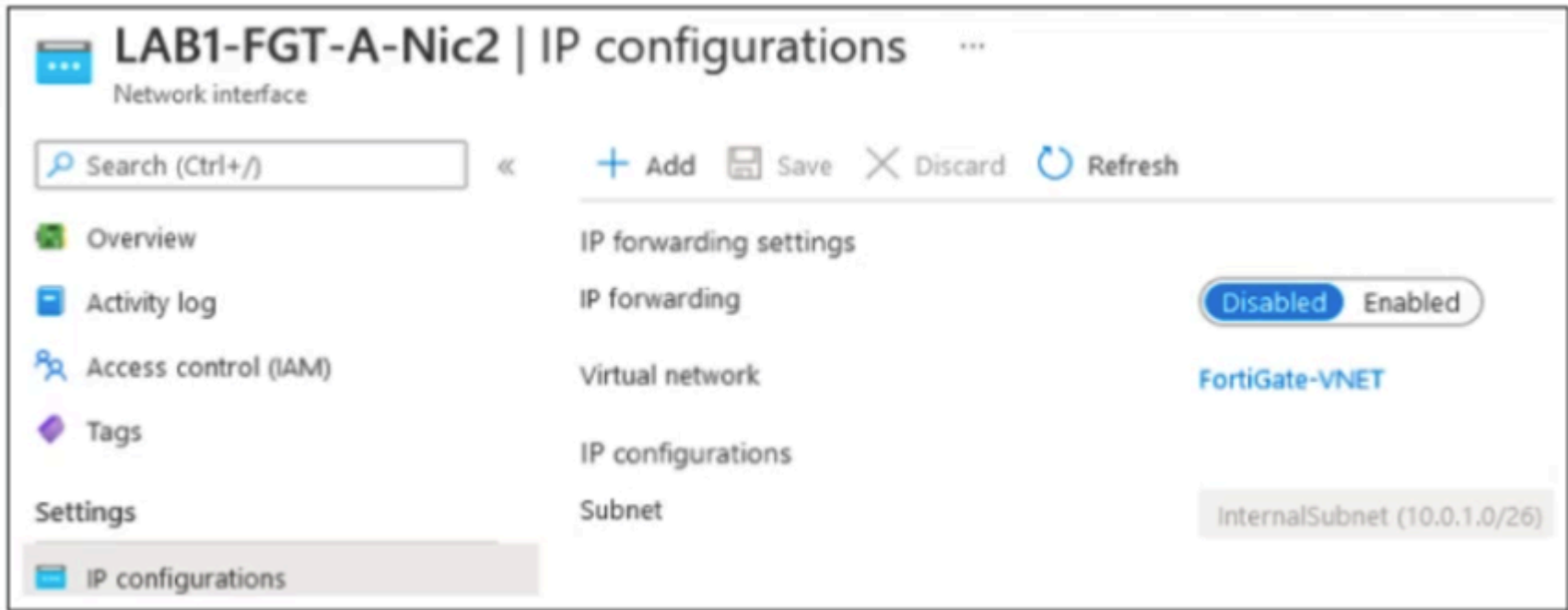
🗨️ 👤 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: A

A is correct here

upvoted 2 times

Refer to the exhibit.



The exhibit shows some of the properties of a virtual NIC that is used by a FortiGate VM deployed in Azure. The virtual NIC shown is connected to a subnet (10.0.1.0/26) with several VMs that will be accessing the internet through the FortiGate VM. Which statement is true for this scenario?

- A. The NIC in the exhibit needs to be assigned a public IP address.
- B. The VMs in the 10.0.1.0/26 subnet can access the internet through FortiGate.
- C. You must change the default gateway on the VMs in the Internal Subnet for this to work.
- D. The parameters of the virtual NIC are not configured correctly.

Suggested Answer: C

Community vote distribution

B (50%)

D (50%)

Powers22 1 month, 3 weeks ago

Selected Answer: D

IP Forwarding is required when routing traffic to other networks like the internet. Without this enabled, internal servers will be unable to access the internet via this network gateway
upvoted 1 times

zufyozirke 2 months, 4 weeks ago

Selected Answer: B

The answer is B
upvoted 1 times

Refer to the exhibits.

FGT connector settings

Azure Connector

Server region

Global

Use managed identity

☐

Directory ID

60b93279-efda-45f5-9c1d-e7f999c7

Application ID

e7ac2b2f-25b1-4e66-96b4-9dbc90e

Client secret

This field is required.

Resource path

☒

Subscription ID

9a359c2e-e035-4d1e-ba17-0b600cb2

Resource group

☒ SxLab

Application registration key

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
FortGateKey	12/31/2299	application secret	

You are configuring an SDN connector for Azure on a FortiGate device You completed all the required steps on the Azure side. While configuring the FortiGate side, you notice that you did not save the client secret used in the Azure App Registration.

What is the quickest way to obtain the value of the client secret?

- A. Create a new resource group
- B. Create a new client secret
- C. Create a new app registration
- D. Create a new external connector for Azure

Suggested Answer: B

Community vote distribution

B (67%)

C (33%)

- Powers22

1 month, 3 weeks ago

Selected Answer: B

Client secret values are not stored in a way that they can be retrieved after creation. To view a client secret's value, you must create a new one and immediately save it. After navigating away from the secret's creation page, the value is no longer accessible.

upvoted 2 times
- zufyozirke

2 months, 4 weeks ago

Selected Answer: C

C is the correct choice

upvoted 1 times

Your organization is in the process of optimizing its Azure network architecture and wants to dynamically manage and exchange routing information between its virtual networks and on-premises networks.


Which Azure service would help to provide a centralized point for efficient route management and dynamic routing?

- A. Azure Virtual WAN
- B. Azure VPN Gateway
- C. Azure ExpressRoute
- D. Azure Route Server

Suggested Answer: *D*

Community vote distribution



  **zufyozirke** 2 months, 4 weeks ago

Selected Answer: D

Must be D

upvoted 2 times

A Linux server was deployed in a protected subnet with a dynamic IP address. A FortiGate VM in the internal subnet provides traffic filtering to it. and you must implement a firewall policy using the IP address of the Linux server.

Which feature could help integrate FortiGate using Linux server tags?

- A. Targets Management
- B. Microsoft Entra ID
- C. Software-defined network (SDN) connector
- D. Service Fabric Cluster

Suggested Answer: C

Community vote distribution



🗨️ 👤 **Powers22** 1 month, 3 weeks ago

Selected Answer: C

SDN will allow the Fortigate to receive dynamic address objects for the protected servers. If they change in Azure, then the FortiGate address object will update accordingly

upvoted 1 times

🗨️ 👤 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: A,B

A and B are correct

upvoted 1 times

Refer to the exhibits.

FortiGate sniffer output

```
FGTlab-FGT-A # diagnose sniffer packet any 'port 80' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 80]
2.727141 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: syn 2787271009
2.727149 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: syn 2787271009
2.727743 port1 in 168.63.129.16.80 -> 10.0.0.4.15048: syn 2252873112 ack 2787271010
2.727791 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252873113
2.727795 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252873113
2.727831 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: psh 2787271010 ack 2252873113
2.727834 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: psh 2787271010 ack 2252873113
2.729649 port1 in 168.63.129.16.80 -> 10.0.0.4.15048: 2252873113 ack 2787271142
2.729670 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252874541
2.729672 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252874541
2.729678 port1 in 168.63.129.16.80 -> 10.0.0.4.15048: psh 2252874541 ack 2787271142
2.729688 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252875391
2.729690 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: ack 2252875391
2.729728 port1 out 10.0.0.4.15048 -> 168.63.129.16.80: fin 2787271142 ack 2252875391
2.729730 sriovslv0 out 10.0.0.4.15048 -> 168.63.129.16.80: fin 2787271142 ack 2252875391
```

FortiGate sniffer output

```
FGTlab-FGT-A # diagnose sniffer packet any 'port 22' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 22]
^C
0 packets received by filter
0 packets dropped by kernel

FGTlab-FGT-A #
FGTlab-FGT-A #
FGTlab-FGT-A #
FGTlab-FGT-A #
```

A high availability (HA) active-active FortiGate with Elastic Load Balancing (ELB) and Internal Load Balancing (ILB) was deployed with a default setup to filter traffic to a Linux server running Apache server.

Ports 80 and 22 are open on the Linux server, and on FortiGate a VIP and firewall policy are configured to allow traffic through ports 80 and 22.

Traffic on port 80 is successful, but traffic on port 22 is not detected by FortiGate.

What configuration changes could you perform to allow SSH traffic?

- A. Configure a customized port under the Frontend IP configuration
- B. Add a new Azure load balancing rule
- C. Include the Linux server in the back-end pool options
- D. Add a new Inbound NAT rule

Suggested Answer: D

Community vote distribution

B (67%)


B,C (33%)

 **Powers22** 1 month, 3 weeks ago

Selected Answer: B

Azure Load Balancer does not directly support defining a port range within a single load balancing rule. Instead, you need to create individual rules for each port you want to forward. For example, if you need to forward traffic for ports 65520 to 65530, you would need to create 11 separate load balancing rules. Inbound NAT rules are generally used to map destination ports to specific VMs in the backend pool rather than listening on additional ports.

upvoted 2 times

 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: B,C

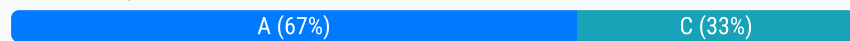
B and C are the answers
upvoted 1 times

Which additional features does Azure Firewall Premium offer compared to Azure Firewall Standard?

- A. Content filtering and threat intelligence integration
- B. Antivirus detection and AI prevention capabilities
- C. Enhanced URL filtering and web categories
- D. Advanced DDoS protection and VPN diagnostics

Suggested Answer: *C*

Community vote distribution



🗲️ 👤 **Powers22** 1 month, 3 weeks ago

Selected Answer: C

- A - this is provided with standard
 - B - Azure Firewall doesn't offer this
 - C - Only Azure Firewall Premium provides ENHANCED URL filtering
 - D - Azure firewalls don't provide this - different service
- upvoted 1 times

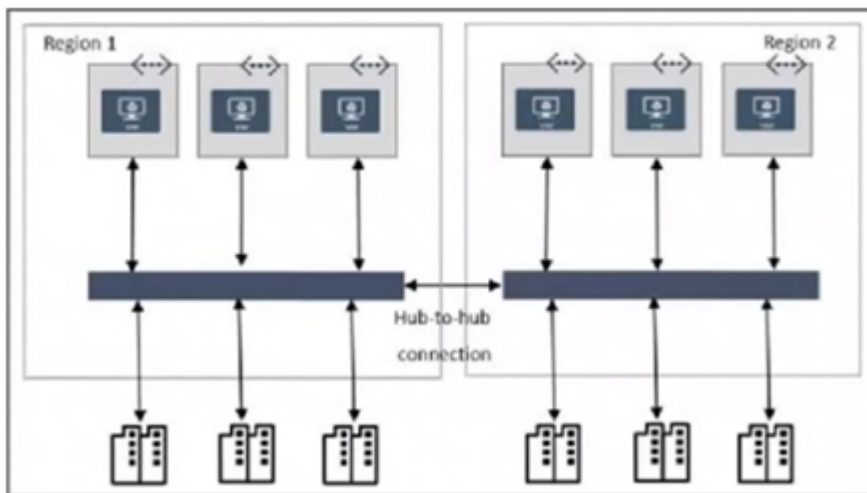
🗲️ 👤 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: A

After reviewing, A is correct

upvoted 2 times

Refer to the exhibit.



Your organization is planning the implementation of a complex hub-to-spoke solution to meet automated large-scale branch connectivity with multiple regions, offering a diverse range of connectivity options.

Which Azure networking service can deliver a solution?

- A. Azure SD-WAN
- B. Azure Virtual WAN
- C. Azure VPN Gateway
- D. Azure Firewall Manager

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: B

Clearly B

upvoted 2 times

You are deploying a site-to-site IPsec VPN connection between your on-premise subnet and your Azure VNets.
What is the most important advantage for using FortiGate at both ends of the tunnel?

- A. It minimizes the need for encryption in transit
- B. It allows scaling based on performance and capacity requirements
- C. It provides consistent security policies and configurations
- D. It reduces the need for troubleshooting due to FortiGate automatic configuration

Suggested Answer: *C*

Community vote distribution



🗉 👤 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: C

C is the right choice
upvoted 1 times


Your organization is planning to deploy FortiWeb in Azure to provide a web application security solution to its web servers. One of the requirements is to have granular control of the number of vCPUs and memory assigned to this resource. Which cloud model could meet this requirement?

- A. Software-as-a-Service (SaaS)
- B. Platform-as-a-Service (PaaS)
- C. Function-as-a-Service (FaaS)
- D. Infrastructure-as-a-Service (IaaS)

Suggested Answer: *D*

Community vote distribution



 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: D

D is correct based on documentation
upvoted 1 times


What is a key distinction between Azure Firewall and FortiGate VM in terms of their primary functions?

- A. Azure Firewall is a cloud-native network security service, while FortiGate VM is a network virtual appliance (NVA) that provides comprehensive security functions.
- B. Azure Firewall focuses on network traffic inspection, while FortiGate VM is primarily a web application firewall.
- C. Azure Firewall is designed exclusively for application layer filtering, while FortiGate VM is suitable for both on-premises and cloud environments.
- D. Azure Firewall and FortiGate VM have identical primary functions, and no features differentiation.

Suggested Answer: A

Community vote distribution



 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: A,C

A and C are correct

upvoted 1 times

Refer to the exhibits, which show the outputs of two commands taken on a Windows VM running in Azure.

IP address configuration

```
C:\windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : 12htgkvlwy3e1kwr2zeco.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::51f1:1be4:a33b:d868%2
IPv4 Address. . . . . : 10.0.1.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.1.1
```

Trace output

```
C:\windows\system32>tracert 10.0.2.4

Tracing route to 10.0.2.4 over a maximum of 30 hops
 1      <1 ms      <1 ms      <1 ms  10.0.2.4

Trace complete.
```

Which statement is true about the device with the IP address 10.0.2.4?

- A. It is reachable through FortiGate in transparent mode
- B. It is provided by Azure for routing traffic among subnets
- C. It is on the same VNET as the Windows VM
- D. It is on the same subnet as the Windows VM

Suggested Answer: C

Community vote distribution

B (50%)

C (50%)

- Powers22

1 month, 2 weeks ago
- Selected Answer: C
- FortiGates in Azure CANNOT run in transparent mode since there is no L2 in Azure
- Azure SDN routers are not pingable
- The IP address of the windows server and the target in the trace route are clearly on different subnets
- This means it must be C - on the same VNET
- upvoted 1 times
- zufyozirke

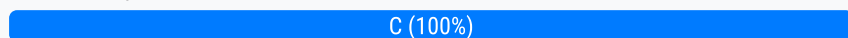
2 months, 4 weeks ago
- Selected Answer: B
- B is the answer
- upvoted 1 times


What is a requirement when you deploy a FortiGate active-active cluster in Azure?

- A. You must assign the public IP address to an Azure load balancer.
- B. You must use unicast FGCP to synchronize the configurations.
- C. You must configure both load balancers to allow administrative access.
- D. You must configure all FortiGate VMs with three or more interfaces.

Suggested Answer: A

Community vote distribution



 **zufyozirke** 2 months, 4 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times